

Confidential

Autorità Garante per la protezione dei dati personali
Piazza di Monte Citorio n. 121
00186 ROMA

Network Transmission and Communications Department

Reference: DCRT/GP/125145

Date: 9 November 2018

Dear Sirs

Re: Submission of clarifications to request for information dated 11 May 2018

I am writing on behalf of Facebook Ireland Limited ("Facebook Ireland") regarding your request for information received on Friday, 11 May 2018 (the "Request") and your follow-up request for information sent on 26 October 2018 regarding our "Ballot" tool (the "Follow Up Request"). We have replied to the Request with three communications dated 21 May, 13 and 15 June 2018 (collectively, the "Reply"). We are writing to respond to the questions in your Follow Up Request and, in the hope that your Office will find it useful, to provide further information relevant to the Request.

For the avoidance of doubt, Facebook Ireland relies on the points already made in the Reply.

We appreciate you keeping the information contained in this response strictly confidential. We respectfully request the opportunity to supplement or amend our response, if needed. Facebook Ireland also respectfully requests that such information be accorded protection from disclosure and that it be kept confidential under all applicable freedom of information laws. Facebook Ireland further requests that you provide the undersigned with notice and an opportunity to be heard in the event that you decide that you will disclose any information provided by Facebook Ireland.

Subject to those general points, we share the information below with you now which are primarily relevant to questions (a) to (d) of the Request, relating to the Cambridge Analytica matter, and questions (h) to (j) of the Request, relating to the access to data of Facebook users by third parties. Please do not hesitate to contact us if you have any further questions or would like clarification on any point.

I. Applicable law and jurisdiction

At the outset, we restate our position that Facebook Ireland is the sole data controller for all EU users of the Facebook service, including Italian users.

We are providing the Reply on a voluntary basis and on the understanding that before the enactment of EU Regulation 2016/679 - "**GDPR**" - the operation of the Facebook service in Europe was governed by Irish data protection laws and subject to regulation by the Irish Data Protection Commissioner ("IDPC"). This would include all matters referenced in the Request relating to facts and circumstances occurring before 25 May 2018.

Since the enactment of the GDPR, under Article 56(1), the IDPC has been the lead supervisory authority with regard to the Facebook service in the EU. In the event that the



Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Curran
Company No. 482932

Authority has any concerns in relation to the cross-border processing conducted by Facebook Ireland under the GDPR, these should be referred to the IDPC as our "sole interlocutor" on such issues under the provisions of Article 56(6).

The concept of the lead supervisory authority acting as sole interlocutor with regard to cross-border processing represents one of the pillars of the GDPR. It aims at achieving uniformity and creating certainty in the interpretation and enforcement of European data protection laws. Any attempt to circumvent the role and competence of the lead supervisory authority would not only be a violation of Article 56, but would mean nullifying the efforts of the GDPR to eliminate this uncertainty and inconsistency. These core concepts are, for example, recognised in Recital (7) of the GDPR, stating that "*Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.*"; and Recital (13) of the GDPR, which notes that "*to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators*".

In this context, this response is therefore provided on a voluntary basis, without prejudice to our rights on jurisdiction and applicable law.

II. Cambridge Analytica

As noted in our letters dated 13 and 15 June 2018, while Dr. Kogan's app, which came to be known as "thisisyourdigitallife", may have accessed data of Facebook users around the world, the evidence currently available to us indicates that he only shared such data with SCL/Cambridge Analytica relating to Facebook users located in the US.

To-date we are aware of no evidence to suggest that Dr Kogan provided any data to Cambridge Analytica or SCL relating to Facebook users located in the EU¹, let alone in Italy. Against this background, we cannot see that the Cambridge Analytica matter has any meaningful data protection or data privacy implications for Facebook users located in Italy.

III. Access to data of Facebook users by third parties

A. Facebook role as an intermediary

The Facebook platform ("Platform") is a platform for sharing - its mission is to give people the power to build community and ultimately to bring the world closer together. People join and use Facebook specifically in order to stay connected with friends and family by sharing information, to discover what's going on in the world, and to share and express what matters to them.

In this context, while it has always sought to educate and inform its users about how the Platform works, it is important to note that Facebook Ireland's role in respect of the sharing of data on the Platform (including user-to-app data sharing) is that of an online intermediary: it facilitates the data-sharing choices freely made by users in respect of the data that they control, consistent with their free speech rights and the public policy imperative to increase the free movement of data (such imperative itself having been expressly recognised in former EU Directive 95/46/EC on the processing of personal data and now confirmed by the GDPR²).

¹ A consideration which we understand was relevant, for example, to the Spanish Data Protection Authority's decision to close their investigations into matters relating to Cambridge Analytica without issuing any sanctions against Facebook Ireland.

² See, for example, Recital 3 and Article 1(2) of EU Directive 95/46/EC and Article 20 of the GDPR.



During the period that Dr Kogan's app operated on the Platform, the choice of what and how much to share, using the technical facilities embodied in the Platform, was, generally speaking, a choice for users, not for Facebook Ireland. Facebook Ireland's users were clearly informed of how their data might be shared with apps and what they could do to exert control over this process.³ Suitable tools were provided through the various privacy controls available to users on the Platform. These included the following (collectively referred to as the "Privacy Controls", and as previously summarized in our response to question (a) in our letter dated 13 June 2018):

- Users decided what information they wanted to share on Facebook in the first place;
- They decided who they wanted the audience to be for any information which was not part of their public profile, for example by limiting the audience to the user only or to a custom selected group of contacts rather than all friends;
- They could choose to share information with all their friends but restrict the ability for their friends' apps to access that information via the granular choices offered in the Apps Others Use settings; or
- They could choose to share information with their friends but comprehensively stop any apps accessing that information via the Platform Opt-Out setting.

We emphasise the following features of the user-to-app data sharing ability which Facebook made available to users:

- (1) Facebook Ireland received no payment as a result of users sharing their data with third party apps;
- (2) The sharing of user data with third party apps that used Facebook Login always occurred at the instigation of those users who were looking to install the relevant app: it was *their* decision to share data with the app that resulted in the app obtaining the data;
- (3) the process by which users share data with apps was in effect a private transaction as between user and app which Facebook Ireland facilitated;
- (4) Facebook Ireland's role in the context of that transaction was always that of an online intermediary: it technically facilitated the data-sharing decisions actively taken by its users. In effect, its role was to respond, on an automated basis, to the data-sharing commands given to it by users in respect of the data that they themselves controlled (which under V1 of Platform included certain data that their friends had chosen to share with them on Facebook, subject to the privacy choices made by those friends as expressed through their Privacy Controls); and
- (5) Facebook Ireland could only provide those technical means in circumstances where the provision of data to the app was made at the express direction of the user installing the app and, under V1, was otherwise authorised by any friends of that user in accordance with their Privacy Controls.

The collection of data through Facebook Login by these independent third-party apps always has been separate to Facebook Ireland's own data collection activities. It was the relevant third-party app developer that requested permission from users to collect data and it did so

³ See the responses to questions (b), (c) and (i) of the Request in our letter dated 15 June 2018



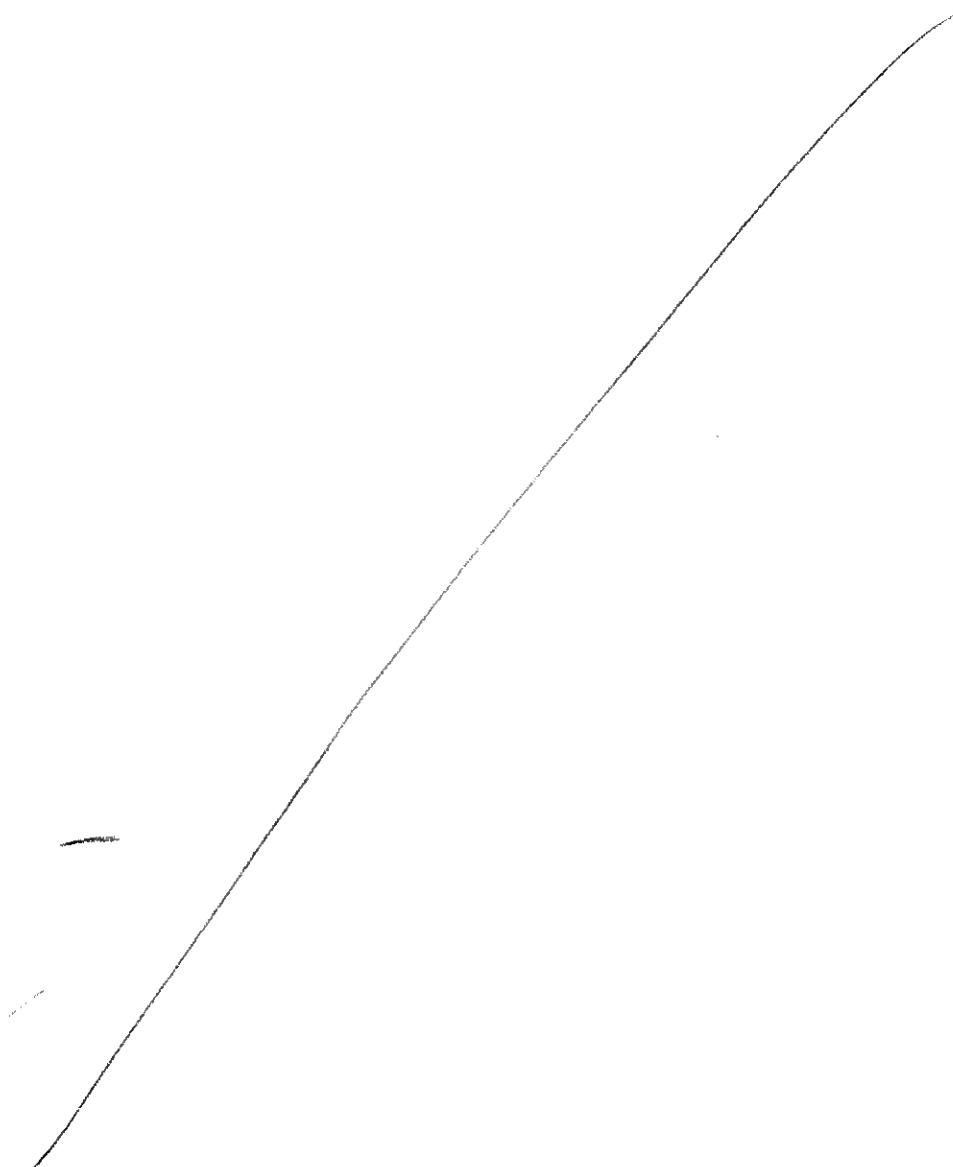
Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lamb, Yvonne Curran
Company No. 462932

subject to: (i) the contractual obligations it owed to its users under the terms and conditions it entered into with those users; and (ii) the statutory obligations to which it was subject under any applicable data protection legislation in its own role as an independent data controller. The legal responsibility and burden of supervising these third parties' use of data was a matter for relevant regulators rather than Facebook Ireland. To conclude otherwise would undermine the concept of data controller, and would also run contrary to the principles set out in EU law protecting online intermediaries.

Nonetheless, out of a desire to go above and beyond its legal responsibilities, in order to provide additional safeguards to its users, Facebook Ireland imposed contractual obligations on third party apps using its Platform via its Terms and Platform Policy. Among other things, this required third party apps to put in place appropriate policies and to comply with applicable privacy laws.⁴ Developers also had to observe appropriate standards and comply with Facebook Ireland's prohibition on selling or licensing user data accessed from users via Facebook Ireland's Platform and on sharing any user data accessed from Facebook users with any ad network, data broker or other advertising or monetization-related service.

B. Monitoring and enforcement



C. Platform and oversight by regulatory authorities

Facebook Ireland has a record of highly engaged, constructive and cooperative engagement with the IDPC as its lead regulator. This includes in respect of the extensive and detailed audit work that the IDPC carried out in 2011 and 2012 to assess Facebook's compliance with applicable data privacy laws (resulting in the 2011 Audit Report⁶ and the 2012 Re-Audit Report⁷). The IDPC commended Facebook Ireland in the course of its 2011/2012 auditing activities for its positive approach and commitment to respecting the privacy rights of its users⁸.

Following the 2011/2012 auditing process, the IDPC was clear that its audit and recommendations arising did not carry any implication that Facebook Ireland's practices were

⁶ <https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf>

⁷ https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

⁸ IDPC 2011 Audit Report, p 3

not in compliance with EU data protection law (as transposed into Irish data protection law).⁹ Indeed, the IDPC notably framed its recommendations as recommendations of best practice, i.e. over and above legal compliance. In reaching its conclusions on user-to-app data-sharing on the Platform, the IDPC was informed by extensive technical reports prepared by an independent expert retained by the IDPC, which included an explanation of how the Platform operated and how users could consent to share friends' data with third-party applications. These technical reports – prepared following extensive direct examination of Facebook systems - were published publicly alongside the IDPC Audit Reports and underpinned the best practice recommendations made by the IDPC. The important point being that there was significant transparency around how Platform operated, the IDPC audit and its findings.

In the context of the 2011/2012 auditing process, the IDPC specifically considered the operation of third-party applications on the Platform. Similar work had also been carried out by other regulators, notably the Canadian Office of the Privacy Commissioner, the US Federal Trade Commission ("FTC") and the Nordic and German data protection authorities. The IDPC noted that the FTC had reviewed the operation of third-party applications on the Platform and the scope of data that third-party applications could seek to access.¹⁰ The IDPC also considered a number of specific issues raised in complaints addressed to the Office by the "Europe-versus-Facebook" group, the Norwegian Consumer Council and by a number of individuals. These complaints included the (incorrect) suggestion that "*users of Facebook are not aware that if a Facebook friend of theirs installs an application, that application has the ability to access that user's friends' basic profile information such as picture, and name.*" These parties were able raise concerns with the IDPC on its initial views as well as on Facebook Ireland's published responses.

The IDPC stated that the operation of third-party apps was a significant focus of its audit work¹¹ and, in light of the complaints received on the issue, it specifically considered how best to ensure that users were able to make informed choices about the data that friends could share with third-party apps.¹² It found that users could already make that choice using their Privacy Controls, but recommended that Facebook Ireland enhance granular choice and control in this area.¹³ Following further changes made by Facebook Ireland, the IDPC subsequently recorded satisfactory adoption of its best practice recommendations, including in the key areas of transparency, user control and data security.¹⁴

We otherwise refer your Office in particular to the following sections of the IDPC Audit Reports:

- Section 3.1 of the 2011 Audit Report - Privacy Policy / Data Use Policy - The IDPC recorded satisfactory responses from Facebook Ireland regarding the simplification and improved prominence of its Privacy Policy. Indeed, the ambition of the IDPC was to secure "*an enhanced ability for users to make their own informed choices based on*

⁹ IDPC 2011 Audit Report, p 4

¹⁰ See FTC 29 November 2011 Complaint, paragraph 9. This noted: "Facebook has designed its Platform such that Platform Applications can access user profile information in two main instances. First, Platform Applications that a user authorizes can access the user's profile information. Second, if a user's "Friend" authorizes a Platform Application, that application can access certain of the user's profile information, even if the user has not authorized that Application. For example, if a user authorizes a Platform Application that provides reminders about Friends' birthdays, that application could access, among other things, the birthdays of the user's Friends, even if these Friends never authorized the application." See also IDPC 2011 Audit Report, page 87.

¹¹ IDPC 2012 Re-Audit Report, page 29

¹² IDPC 2012 Re-Audit Report, page 31

¹³ IDPC 2012 Re-Audit Report, page 31

¹⁴ 2012 Annual Report, page 3 and page 19.

https://www.dataprotection.ie/documents/annualreports/Annual_Report_2012.pdf



Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Cunnane
Company No. 462932

*the available information*¹⁵. In the 2012 Re-Audit Report, the IDPC recorded that Facebook Ireland had made changes to the "just in time" provision of information to users, meaning that "*when a user is making a choice or asked to make a choice about how they wish their personal data to be used that they are presented with relevant understandable information at that time on which to base their choice*"¹⁶. A full discussion can be found at section 3.1 of the 2011 Audit Report and pages 13 to 15 of the 2012 Re-Audit Report.

- Section 3.6 of the 2011 Audit Report - Third-party Applications - The IDPC recorded in its 2012 Audit Report that the operation of third-party applications "was a significant focus of our December [2011] Audit"¹⁷ and that Facebook Ireland had satisfactorily implemented the majority of the IDPC's recommendations. A full discussion can be found at section 3.6 of the 2011 Audit Report and pages 33 to 34 of the 2012 Re-Audit Report.
- Key recommendations and conclusions of the IDPC Audit Reports are repeated below for ease of reference.
 - Recommendation 1: Users must be empowered via appropriate information and tools to make informed decisions when granting access to their data to third-party applications. (The IDPC made particular note that Facebook provided clear information at a time that was prior to the installation of Dr Kogan's app, commenting, "*we consider that the above developments have provided a means for users to exercise choice based on clear information prior to taking a decision to install an app*").¹⁸
 - Recommendation 4: Facebook should check whether the links to the privacy policies of third-party applications are live. "*We were pleased therefore that FB-I adopted this recommendation and brought forward an internal tool which ensured that all applications available from the site had an active privacy policy link*".¹⁹
 - "*Conclusion: We verified that it was not possible for an application to access personal data over and above that to which an individual gives their consent or enabled by the relevant settings.*"²⁰
 - Section 3.9 of the 2011 Audit Report - Data Security - In their 2011 Audit Report, the IDPC noted that they had devoted "significant focus during the audit to assessing security issues".²¹ Indeed, the IDPC further recognised that Facebook too "*places an enormous and ongoing focus on the protection and security of user data*".²² A full discussion can be found at paragraph 3.9 of the 2011 Audit Report and pages 39 to 41 of the 2012 Re-Audit Report.

It is surprising that your Office appears to be suggesting, some seven years later, that it now has concerns regarding the operation of Platform from 2011/2012 onwards. This is particularly so given that: (a) the IDPC did not conduct its review in isolation and actively consulted with

¹⁵ IDPC 2011 Audit Report, page 42

¹⁶ IDPC 2012 Re-Audit Report, page 14

¹⁷ IDPC 2012 Re-Audit Report, page 29

¹⁸ IDPC 2012 Re-Audit Report, page 30

¹⁹ IDPC 2012 Re-Audit Report, page 30

²⁰ IDPC 2012 Re-Audit Report, page 30

²¹ IDPC 2011 Audit Report, page 107

²² IDPC 2011 Audit Report, page 108



EU Article 29 Working Party group members; and (b) detailed information concerning user-to-app data sharing on the Platform (including information as to the scope of the data that third-party applications could seek to access) was published by the IDPC in 2011.

The IDPC summarised the result of the IDPC Audit Reports as follows in its 2012 Annual Report (emphasis added):

"In 2011, a major audit of Facebook Ireland (FB-I) was conducted, the report of which was published in December 2011. Arising from the audit, FB-I agreed to a wide range of "best practice" improvements with a formal review of progress to take place in July 2012.

In September 2012, the Office published the outcome of our review of Facebook Ireland's (FB-I) implementation of recommendations made in our Audit.

The Review found that the great majority of the recommendations were fully implemented to our satisfaction, particularly in the following areas:

- *The provision of better transparency for the user in how their data is handled,*
- *The provision of increased user control over settings,*
- *The implementation of clear retention periods for the deletion of personal data or an enhanced ability for the user to delete items,*
- *The enhancement of the user's right to have ready access to their personal data and the capacity of FB-I to ensure rigorous assessment of compliance with Irish and EU data protection requirements.*

Those recommendations which were not implemented by FB-I as of that time were highlighted with a clear timescale for implementation listed. A deadline of 4 weeks for those matters to be brought to a satisfactory conclusion was set and FB-I progressed those matters to our satisfaction within the four week period. The Office continues to maintain an ongoing dialogue with FB-I on the data protection implications of all new services as these are rolled-out.

Throughout the year the Office consulted extensively with colleagues in other Data Protection Authorities on matters which were arising in the context of the Audit process and matters that were of concern or interest to colleagues more generally. In so far as possible we sought to take these issues on board and to achieve satisfactory outcomes. This arose from our recognition that, while we had lead responsibility for the supervision of Facebook in Europe via its Irish establishment, that it was necessary to fully consult with and take account of the views of colleagues whose citizens had concerns about aspects of Facebook's use of their personal data."

The upshot of these conclusions is that, by the end of the audit process, the IDPC regarded Facebook Ireland's approach to transparency, control and data security on Platform as legally unobjectionable. As may be expected, Facebook Ireland relied on these conclusions moving forward, as they were properly entitled to do.

It is important to consider in this context that, in order to guarantee the free movement of data within Europe, which was itself a fundamental pillar of the Directive (and now the GDPR), regulators should be striving to discharge their regulatory duties in a highly concordant manner. Any other approach to regulatory enforcement within the EU risks having a significant chilling effect on the achievement of data mobility within Europe and is otherwise unfair to data controllers, who are entitled to assume that EU regulators will generally themselves apply data protection laws consistently and uniformly across the EU.



Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private limited company
Directors: Gareth Lambe, Yvonne Cummins
Company No. 462932

For completeness we note that, as you will be aware, the office of the UK Information Commissioner ("ICO") has recently issued a penalty to Facebook in connection with the Cambridge Analytica matter. Facebook Ireland is currently reviewing the ICO's decision, and would be entitled to challenge that penalty before the English Information Tribunal on the basis that it is fatally tainted by multiple serious errors of fact and law, including not least the ICO's failure to take into account the conclusions reached by the IDPC (in consultation with other EU data protection authorities) in the context of its review of Facebook Ireland's approach to user-to-app data sharing explained above.

IV. The Follow Up Request

As an initial point with regard to the questions raised in the Follow Up Request, we should clarify the purpose of our Ballot tool, as well as the separate initiatives that took place as part of the 2018 Italian elections. This is because it appears from the summary provided in your letter containing the Follow Up Request that there may be some confusion in this regard.

Ballot was a tool that was made available to Italian users in order to make it easier for them to access information about the candidates in their electoral district. In addition to facilitating access to candidate information – and following collaboration with the Ministry of the Interior, the Presidency of the Council of Ministers, and various other organisations and candidates across the country – Ballot also included a video tutorial to educate users about new voting requirements and new electoral laws that were being introduced in Italy.

The tool was made available for use on an "opt-in" basis, meaning it was entirely optional for users as to whether they wanted to engage with the product or not.

We wish to emphasize that Ballot was launched solely as a civic education and engagement tool, as part of our commitment to supporting an informed and civically engaged community on our platform. The tool was not in any way launched for the purposes of "monitoring of electoral behaviour", contrary to what is stated in your letter. In fact, the tool was specifically architected not to record information about how individual users may have voted in the election.

Separately, and as a distinct initiative from our Ballot product, as another part of our commitment to supporting civic engagement on our platform in the 2018 election, we issued an Election Day reminder in Italian users' News Feeds. This reminder provided users with information about how and where to vote, and also gave them the option to share that they had voted. We also made election results available on Facebook after the polls had closed; and after the new government was formed we provided an in-app notification enabling users to learn who their current and new representatives were.

In that context, the specific questions raised in the Follow Up Request are answered below:

(a) What processing has been carried out with respect to the personal data acquired with the log files relating to the access of individual users to the profiles of candidates and their possible confirmation of having voted?

As explained in our response dated 21 May 2018, we obtained basic logs of users' actions if they chose to use Ballot. This information was only used for the purposes of generating aggregated engagement metrics – i.e. generalised metrics providing an overview of how Facebook users as a whole were engaging with the product, and not any sort of analysis as to how specific individuals may have used the product. These aggregated metrics helped us to understand how the product was being used and how it could be improved to make it more useful generally for users in future elections, both in Italy and other countries. The underlying log data used to create these aggregated metrics was deleted after 90 days.



Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Curran
Company No. 462932

With regard to the second part of your question – i.e. what processing was carried out with respect to the personal data contained in any user posts confirming that they had voted – we did not monitor the content of any such posts that users chose to make in order to assess or understand their voting decisions in any way. The purpose of the prompts we sent to users was simply to encourage civic engagement on our platform. As with all of their posts, users can see what they have posted previously and delete those posts at any point, including through their Activity Log.²³

(b) What was the purpose for which such processing was carried out?

See our answer to (a) above.

(c) What data was the "postal address" made up of (the address in its entirety or only the postcode)?

If a user wished to use the Ballot product, they could enter their full postal address. This was required in order to ensure their constituency was correctly identified and they were shown the correct candidate information – for example, just providing a postcode would have been insufficient to reliably ascertain a user's constituency. As explained in our previous letter, users were given full control over the address information they chose to provide in this way (assuming they chose to engage with the Ballot product in the first place). They were able to skip entering it or, once they had learned about their local candidates, they could remove or edit it.

(d) What information has been provided to the data subjects with regards to the abovementioned processing operations?

As explained in our previous response, our Data Policy explained to users what information we collected and how we used it. For example, the Data Policy in force at the time of the 2018 elections stated as follows:

I. What kinds of information do we collect?

Depending on which Services you use, we collect different kinds of information from or about you.

- *Things you do and information you provide. We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.*

[...]

II. How do we use this information?

We are passionate about creating engaging and customized experiences for people. We use all of the information we have to help us provide and support our Services. Here's how:

²³ <https://www.facebook.com/help/289066827791446>



Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Cunnane
Company No. 462932

- **Provide, improve and develop Services.** We are able to deliver our Services, personalize content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things you're connected to and interested in on and off our Services. [...] We conduct surveys and research, test features in development, and analyze the information we have to evaluate and improve products and services, develop new products or features, and conduct audits and troubleshooting activities.

[...]

III. How is this information shared?

Sharing On Our Services

People use our Services to connect and share with others. We make this possible by sharing your information in the following ways:

- **People you share and communicate with.** When you share and communicate using our Services, you choose the audience who can see what you share. For example, when you post on Facebook, you select the audience for the post, such as a customized group of individuals, all of your Friends, or members of a Group. Likewise, when you use Messenger, you also choose the people you send photos to or message. Public information is any information you share with a public audience, as well as information in your Public Profile, or content you share on a Facebook Page or another public forum. Public information is available to anyone on or off our Services and can be seen or accessed through online search engines, APIs, and offline media, such as on TV. In some cases, people you share and communicate with may download or re-share this content with others on and off our Services. When you comment on another person's post or like their content on Facebook, that person decides the audience who can see your comment or like. If their audience is public, your comment will also be public.

[...]

IV. How can I manage or delete information about me?

You can manage the content and information you share when you use Facebook through the Activity Log tool. You can also download information associated with your Facebook account through our Download Your Information tool.

We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.

You can delete your account any time. When you delete your account, we delete things you have posted, such as your photos and status updates. If you do not want to delete your account, but want to temporarily stop using Facebook, you may deactivate your account instead. To learn more about deactivating or deleting your account, click here. Keep in mind that information that others have shared about you is not part of your account and will not be deleted when you delete your account.

The current Data Policy, which has since been updated, can be found here: <https://www.facebook.com/policy.php>.



Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private limited company
Directors: Gareth Limbo, Xanthe Curran
Company No. 467932

As also explained in our previous response, Ballot provided specific "just-in-time" in-product disclosures to users at the moment when they were presented with the option of entering their address. This included instructions about how users could edit or remove this information at any time, as well as a "Learn More" link for those users who were interested in finding out more detailed information regarding why Facebook needed their address information for Ballot and how that information would be used. Similar information was also generally available in our Help Centre.²⁴

e) What is meant by the expression "aggregate engagement matrices" (your reply dated May 21st, 2018), if possible providing examples?

As explained in our response to question (a) above, aggregate engagement metrics are metrics which provide an overview of how Facebook users as a whole engage with a product. They are not any sort of analysis as to how specific individuals may have used the Ballot product. These aggregate engagement metrics helped us to understand how the Ballot product was being used generally, and how it could be improved to make it more useful for users in future elections. For example, we analysed the average amount of time spent on different features in the product, as an indicator of whether users generally were finding those features useful or interesting. This analysis enabled us to then make more informed decisions about which parts of the product would benefit from improvements.

f) Finally, with reference to the expression used in the FAQ "*information you provide may also be used for future Facebook features*", which are in detail the personal data requested from users "for future Facebook features" and what are the purposes for which such personal data may be retained?

We currently only use address information provided by Italian Facebook users through their use of Ballot for the purposes of government and election features on Facebook. The only such features launched in Italy to-date which utilised this address information – if users chose to provide it – are Ballot and the in-app notification that was issued on mobile after the 2018 election inviting users to find and follow their newly elected representatives, as explained above.

I hope that this information is helpful in addressing the questions you have raised. Please do not hesitate to contact us if you require anything further.

Please find enclosed a courtesy Italian translation of this letter.

Yours faithfully

and Limited

2909



Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Garbhá Lambe, Yvonne Cummins
Company No. 492972